TECHNOLOGY TIMES

INSIDER TIPS TO MAKE YOUR BUSINESS RUN FASTER, EASIER AND MORE PROFITABLY SINCE 2003

August 2024

What Do You Do When a Company Compromises Your Data?

With the rise in cyber attacks worldwide, you've likely received more than one notification from a company you work with informing you that your data has been compromised in a breach. While there are steps we can take as consumers to protect ourselves, sometimes we can't control when a company that promised to protect our personal data gets hacked.

In 2023, Statista reported that 52% of all global organization breaches involved customers' personal identifiable information (PII), making your personal data – addresses, numbers, names, birth dates, SSNs, etc. – the most commonly breached type of data. A recent example is ChangeHealthcare, breached in February of this year. Due to the breach, it's estimated that one-third of Americans – possibly including you – had sensitive information leaked onto the dark web.

So now what? What do you do when you receive a letter in the mail from your healthcare provider or favorite retail store admitting, "Whoops, we got breached." It's more than upsetting to think that your data is now in the hands of criminals.

When sensitive information leaks, you'll have to do some recon to protect your accounts from suspicious activity. Follow these seven steps to stop the bleeding after a company fails to protect your data from being compromised.

WHAT TO DO AFTER YOUR DATA'S BEEN LEAKED

1. First, make sure the breach is legit.

One ploy that hackers use to get our data is to impersonate popular companies and send out fake e-mails or letters about an alleged breach. Whenever you get a notification like this, go to the company's website or call the company directly. Do NOT use

Continued on pg.2

20 YEARS

This monthly publication provided courtesy of David Luft, CEO of LDD Consulting, Inc.

Our Mission:

We promise to provide knowledgeable, courteous and prompt service. We care as much about your business as you do. If you are not completely satisfied, be sure to let us know. If we cannot resolve the issue, we will refund your money.

... continued from cover

information in the letter or e-mail because it could be fake. Verify that the company was hacked and which of your data may have been compromised. Try to get as much information as possible from the company about the breach. When did it happen? Was your data actually impacted? What support is the company offering its customers to mitigate the breach? For example, some companies offer yearlong free credit monitoring or identity fraud prevention.

Though companies are tasked with safeguarding customer data, breaches are inevitable. Taking proactive steps can help you mitigate the damage and protect yourself in the aftermath.

2. Figure out what data was stolen.

After speaking directly with the company, determine what data was stolen. Credit cards can be easily replaced; Social Security numbers, not so much. You'll want to know what was compromised so you can take the necessary steps to monitor or update that information.

3. Change passwords and turn on MFA.

After a breach, you'll want to quickly update to a new, strong password for the breached account and any account with the same login credentials. Additionally, if you see an option to log out all devices currently logged in to your account, do that.

While you're doing that, make sure you have multifactor authentication turned on in your account or privacy settings so that even if a hacker has your login, they can't access your account without your biometric data or a separate code.

4. Monitor your accounts.

Even after changing your passwords, you should keep a close eye on any accounts linked to the breach. Watch out for any account updates or password changes you didn't authorize. They may be a sign of identity theft. If your credit card number was stolen, pay attention to your bank and financial accounts and look for unusual activity, such as unexpected purchases.

5. Report it.

If you're not sure a company knows it's been breached or you've experienced fraud due to a breach, report it to relevant authorities like local law enforcement or the Federal Trade Commission. They can provide guidance and next steps on how to protect your identity.

6. Be aware of phishing attempts.

Often, after data leaks, hackers use the information about you they stole to send you phishing e-mails or calls to trick you into giving away even *more* sensitive information. Be very wary of any e-mails you weren't expecting, especially those that request personal or financial information, and avoid clicking on any links or attachments.

7. Consider identity theft and data breach protection.

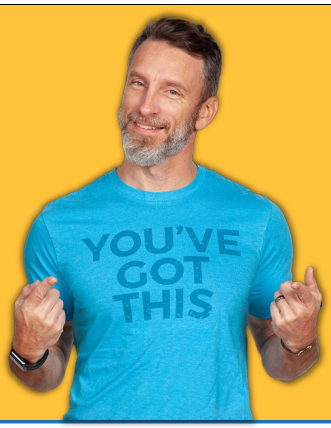
Consider identity theft protection after a breach, especially when highly sensitive data is stolen, like your SSN. It's a time-consuming process to replace a Social Security card. In the meantime, criminals could be using it to impersonate you. Identity theft and data breach protection help monitor your credit or other accounts, protect your identity and notify you when your data appears on the dark web.

While companies are responsible for protecting customer information, breaches can and will still occur. By following the steps above, you can minimize a breach's impact on your life. Ultimately, we must all contribute to protecting our information in an increasingly risky digital world.

TECH TIP:

Do NOT Use FREE VPNs!

Mike Michalowicz Explains How to Build a Team That Cares About Your Company's Success as Much as You Do



Early in his career, Mike Michalowicz eagerly announced a $10 million revenue goal to his team, hoping it would be a visionary moment. Instead, he faced unexpected silence. A colleague told him, "If we hit $10 million, you get the bigger house and new car. What about our vision?" This feedback was a turning point for Michalowicz, leading him to focus on becoming a great leader.

Today, Michalowicz, author of *Profit First*, *Get Different, The Pumpkin Plan*, and other essential business books, helps leaders build and retain motivated teams that share the company's vision, leading to faster growth and a thriving work environment.

HOW TO BUILD AN UNSTOPPABLE TEAM

Most leaders tell their team what to do. Great leaders ask their team what they *could* do.
One of the Baltimore Museum of Art's most successful exhibits was curated by 17 museum guards. The idea came from a conversation between a curator and a guard around what the guard did day-to-day. He revealed how much he learned about the art from patrons and what interested them. Museum leaders quickly learned this wasn't unique to the one guard, and a group was assembled to create "Guarding the Art." Michalowicz explains that great leaders encourage ownership by asking, *"What could we do?"* rather than always telling their employees what to do.

Great leadership assembles and unifies.
The movie *The Boys in the Boat* recounts how an inexperienced US rowing team won gold in the 1936 Olympics. The leader helped the team connect, communicate and work together to win against all odds. He fostered deep trust within the team, which Michalowicz says distinguishes great leadership in any circumstance.

Great leaders follow a FASO model.
Michalowicz's research and experience in leadership led to his four-part model he calls "FASO" to assemble an unstoppable team.

⇒ **F – "Fit."** When hiring a new team member, they must be an ideal fit for the organization, and the organization must be an ideal fit for them.
⇒ **A – "Ability."** Great leaders look for people's raw potential. Do they have curiosity, desire and a thirst for the role? That's what great leaders hire and recruit for, not simply experience and innate ability.
⇒ **S – "Safety."** Great leaders account for their team's physical, relational and financial safety. They ensure that people feel safe in how they are treated and where they work, they have a transparent financial culture and they educate their team on personal finances.
⇒ **O – "Ownership."** "When we're forced to comply, we'll *seek* to defy," Michalowicz says. Great leaders encourage their team to personalize, gain intimate knowledge of and control aspects of their work.

Above all, Michalowicz says, "No one cares how you care; they care THAT you care." Show your team you care by working to incorporate these great leadership approaches in your organization.

Client Spotlight

On the Fence about Choosing LDD? Do it… You'll be happy!

Using LDD's VoIP services has been great. The ability to handle office calls on personal cell phones and their excellent tech support are valuable benefits. David and his staff are patient, thorough, and prompt in customizing our phone needs. We love the personal service and that LDD is a local company with excellent customer service. We happily recommend LDD for VoIP services.

Tina M. Reames
President
CSR Architects
Albuquerque

Are You Using This Helpful Google Calendar Hack?

It's a bit embarrassing when you log in to your computer at 9:00 a.m. only to realize you missed the all-team Zoom meeting at 8:30 a.m. Thankfully, Google Calendar offers a helpful hack: daily agendas. With this feature, you can send yourself a daily agenda first thing in the morning so you know everything planned for the day. To set it up, log into your Google account and go to Settings. Find "Settings for my calendars" > "Other notifications" > "Daily agenda." The default is set to "None," so click on it and change it to "Email." Now you have a daily agenda automatically sent to your inbox before you even get out of bed!

Making Technology Work for You
2420 Midtown PL NE, Suite K
Albuquerque, NM 87107

PRST STD
US POSTAGE
PAID
ABQ, NM
PERMIT 1187

Return Service
Requested

«Name»
«Company Name»
«Street Address 1» «Street Address 2»
«City», «State» «Postal Code»

Inside This Issue

Don't Make This Mistake With Your Home's Smart Tech

Smart devices, like door cams and AI assistants, are integral to our homes. Unlike older devices, they need ongoing attention due to their Internet connectivity, which makes them hacker targets. Hackers can exploit weak passwords to commit crimes, such as spying through home cameras. Follow these steps to secure your smart device.

PROS AND CONS OF SMART DEVICES

Unprotected devices, like an indoor camera with a default password, allow hackers to access sensitive information such as your address, birth date, email, and phone number. Criminals can use this data to build profiles and launch targeted attacks. A family in Mississippi experienced a hacker taunting their daughter through a ring camera. To avoid such incidents, follow these security steps:

Steps to Keep Your Smart Home Safe

1. *Change the Default Login Information Immediately:* Default passwords are easy targets for hackers. Change them to stronger passwords right away.
2. *Secure Your WiFi:* If your WiFi password is old or reused on other accounts, change it to a stronger one.
3. *Enable MFA:* This adds an extra layer of security, making it much harder for hackers to gain access.
4. *Regularly Update the Device:* Updates fix security issues and add new features. Don't skip them. If your device doesn't update automatically, set reminders to check for updates periodically.
5. *Consider Separate Networks:* Use a guest network for your smart devices, separate from the one your phones or laptops use. This limits access to more valuable information if a smart device is hacked.

The biggest mistake is thinking smart devices are "set and forget." These tips will help ensure your device isn't an open door for criminals.